

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-346210
 (43)Date of publication of application : 14. 12. 1999

(51) Int. Cl. H04L 9/08
 G09C 1/00
 H04L 9/32

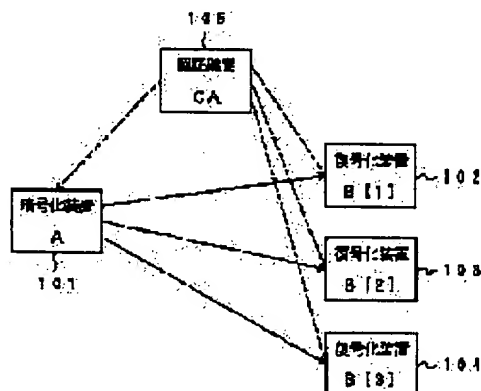
(21)Application number : 10-152866 (71)Applicant : NIPPON TELEGR & TELEPH
 CORP <NTT>
 (22)Date of filing : 02.06.1998 (72)Inventor : ARAKAWA MEGUMI
 WATABE KATSUTOSHI
 TAMANO DAISUKE

(54) ENCRYPTION METHOD AND DEVICE, DECODING METHOD AND DEVICE, RECORD MEDIUM RECORDING ENCRYPTION PROGRAM, RECORD MEDIUM RECORDING DECODING PROGRAM, METHOD FOR ELECTRONIC SIGNATURE AND METHOD FOR AUTHENTICATING ELECTRONIC SIGNATURE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the encryption method and device and the decoding method and device by which a group encryption for a public key system is realized while keeping a form of one privacy key possessed by one person and one public key open to a certificate agency(CA) so as to attain secure and simple key delivery and to simply generate an optional group, and to provide the record medium recording an encryption program and the record medium recording a decoding program.

SOLUTION: The encryption method that is used when a file sender distributes files to one or plural recipients includes at least a step where the sender encrypts the files by using a symmetric key, a step where the sender encrypts the symmetric key by using a private key of the sender and a public key of the recipients, and a step where the sender sends the encrypted files and the encrypted symmetric key.



LEGAL STATUS

[Date of request for examination] 14. 12. 2000
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) ; 1998, 2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-346210

(43) 公開日 平成11年(1999)12月14日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 9/08

G 0 9 C 1/00

H 0 4 L 9/32

6 6 0

H 0 4 L 9/00

G 0 9 C 1/00

H 0 4 L 9/00

6 0 1 A

6 6 0 D

6 0 1 E

6 7 5 D

審査請求 未請求 請求項の数36 O L (全 25 頁)

(21) 出願番号

特願平10-152866

(22) 出願日

平成10年(1998)6月2日

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 荒川 恵

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 渡部 勝年

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 玉野 大祐

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

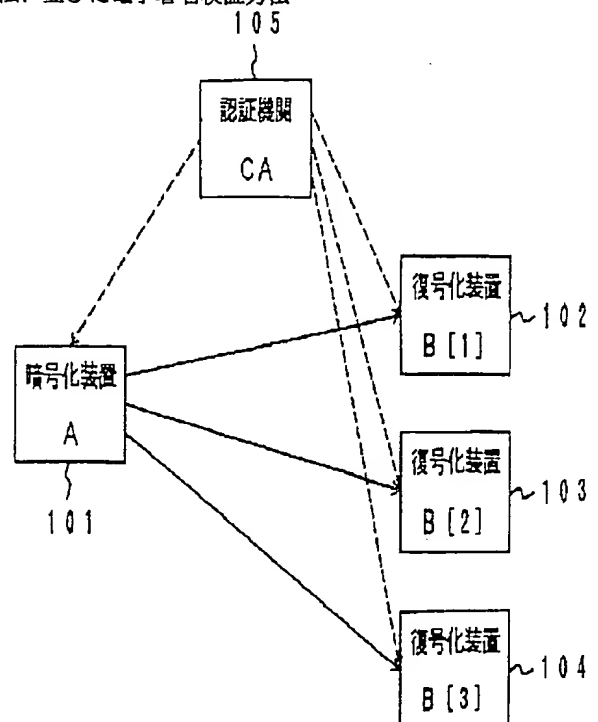
(74) 代理人 弁理士 鈴江 武彦 (外2名)

(54) 【発明の名称】 暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法

(57) 【要約】

【課題】本発明の課題は、個人が持つ1つの秘密鍵、認証機関 (CA) に公開されている1つの公開鍵という形態のままで公開鍵方式のグループ暗号を実現することにより、鍵配送が安全でかつ簡単であり、さらに任意のグループを簡単に作成する事ができる暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、並びに復号化プログラムを記録した記録媒体を提供することにある。

【解決手段】本発明は、ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする暗号化方法。



【特許請求の範囲】

【請求項1】 ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、
対称鍵を用いて該ファイルを暗号化するステップと、
該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、
前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする暗号化方法。

【請求項2】 ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、
対称鍵を用いて該ファイルを暗号化するステップと、
該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、
前記暗号化したファイルと前記暗号化した対称鍵を記録媒体に記録して受信者へ渡すステップとを少なくとも持つことを特徴とする暗号化方法。

【請求項3】 前記ファイルに関する情報を対称鍵を用いて暗号化するステップを持つことを特徴とする請求項1又は2記載の暗号化方法。

【請求項4】 前記ファイル内容及びファイルに関する情報に電子署名情報を付与することを特徴とする請求項3記載の暗号化方法。

【請求項5】 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする請求項1、2、3又は4記載の暗号化方法。

【請求項6】 暗号化されたファイル及び対称鍵を復号化する復号化方法であって、
前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、
該復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。

【請求項7】 暗号化されたファイル及び対称鍵を復号化する復号化方法であって、
前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、
該復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップと、
復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定するステップを持つことを特徴とする復号化方法。

【請求項8】 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする請求項6又は7記載の復号化方法。

【請求項9】 対称鍵を発生する対称鍵発生手段と、
この対称鍵発生手段で発生した対称鍵でファイルを暗号

化するファイル暗号化手段と、

前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、
この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルを連結する連結手段とを具備することを特徴とする暗号化装置。

【請求項10】 対称鍵を発生する対称鍵発生手段と、
この対称鍵発生手段で発生した対称鍵でファイルを暗号化するファイル暗号化手段と、

前記対称鍵発生手段で発生した対称鍵でファイルに関する情報を暗号化するファイル情報暗号化手段と、
前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、
この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルと前記ファイル情報暗号化手段で暗号化したファイルに関する情報を連結する連結手段とを具備することを特徴とする暗号化装置。

【請求項11】 ファイル内容及びファイルに関する情報に送信者の署名用秘密鍵で電子署名情報を付与する電子署名手段を具備することを特徴とする請求項9又は10記載の暗号化装置。

【請求項12】 暗号データから暗号化された対称鍵と暗号化されたファイルを分離する暗号データ分離手段と、

この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、

この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。

【請求項13】 暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、

この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、

この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、

このファイル復号化手段で復号化された電子署名付ファイルを送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。

【請求項14】 暗号データから暗号化された対称鍵と暗号化されたファイルに関する情報と暗号化されたファイル内容を分離する暗号データ分離手段と、

この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、

この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイル情報を復号化するファイル情報復号化手段と、
前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。

【請求項15】 暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルに関する情報と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、

この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、

この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルに関する情報を復号化するファイルに関する情報復号化手段と、

前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、

このファイル復号化手段で復号化された電子署名付ファイルと前記ファイル情報復号化手段で復号化された電子署名付ファイル情報を送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。

【請求項16】 復号化されたファイル情報に基づいて所定のファイルを選択して復号化するファイル選択手段を具備することを特徴とする請求項14又は15記載の復号化装置。

【請求項17】 ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化プログラムを記録した記録媒体であって、

対称鍵を用いて該ファイルを暗号化する手順、

該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化する手順、

前記暗号化したファイルと前記暗号化した対称鍵を送信する手順を実行させるための暗号化プログラムを記録した記録媒体。

【請求項18】 前記ファイルに関する情報を対称鍵を用いて暗号化する手順を実行させるためのプログラムを記録したことを特徴とする請求項17記載の暗号化プログラムを記録した記録媒体。

【請求項19】 前記ファイル及びファイルに関する情報に電子署名情報を付与するためのプログラムを記録したことを特徴とする請求項18記載の暗号化プログラムを記録した記録媒体。

【請求項20】 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする請求項1

7、18又は19記載の暗号化プログラムを記録した記録媒体。

【請求項21】 暗号化されたファイル内容又はファイルに関する情報及び対称鍵を復号化するためのプログラムを記録した記録媒体であって、

前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化する手順、

該復号化された対称鍵を用いて前記暗号化されたファイル内容又はファイルに関する情報を復号化する手順を実行させるための復号化プログラムを記録した記録媒体、

【請求項22】 前記復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定する手順を実行させるためのプログラムを記録したことを特徴とする請求項21記載の復号化プログラムを記録した記録媒体。

【請求項23】 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする請求項21又は22記載の復号化プログラムを記録した記録媒体。

【請求項24】 ファイルの所有者が複数の閲覧者（所有者を含む）へ該ファイルを暗号化する方法であって、対称鍵を用いて前記ファイルを暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、

前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【請求項25】 ファイルの所有者が複数の閲覧者（所有者を含む）へファイルの内容と該ファイルに関する情報を暗号化する方法であって、

該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、

対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、

該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、

前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【請求項26】 ファイルの所有者が複数の閲覧者（所有者を含む）へ該ファイルを暗号化する方法であって、前記所有者が前記閲覧者の情報を任意のグループに分けて管理するステップと、

該グループから、前記グループに属する閲覧者の情報を抽出するステップと、

前記閲覧者の情報から前記閲覧者の公開鍵を抽出する

ステップと、

対称鍵を用いて前記ファイルを暗号化するステップと、
該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、
前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【請求項27】 ファイルの所有者が複数の閲覧者（所有者を含む）へファイル内容と該ファイルに関する情報を暗号化する方法であって、
前記所有者が前記閲覧者の情報を任意のグループに分けて管理するステップと、
該グループから、前記グループに属する閲覧者の情報を抽出するステップと、
前記閲覧者の情報から前記閲覧者の公開鍵を抽出するステップと、
該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、
対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、
該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、
前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。
【請求項28】 暗号化したファイルと暗号化済対称鍵全てを結合したものを復号化する方法であって、
前記暗号化したファイルと暗号化済対称鍵全てを結合したものから、前記暗号化したファイルと暗号化済対称鍵全てを分離するステップと、
所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、
該復号化された対称鍵を用いて該暗号化したファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。

【請求項29】 暗号化したファイル内容と暗号化したファイルに関する情報と暗号化済対称鍵全てを結合したものを復号化する方法であって、
前記暗号化したファイル内容と前記暗号化したファイルに関する情報と暗号化済対称鍵全てを結合したものから、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と暗号化済対称鍵全てを分離するステップと、
所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、
該復号化された対称鍵を用いて該暗号化したファイル内容と該暗号化したファイルに関する情報を復号化するステップと、

該復号化されたファイル内容と該復号化されたファイルに関する情報を結合し前記ファイルを再構成するステップとを少なくとも持つことを特徴とする復号化方法。

【請求項30】 復号化されたファイルに関する情報に基き、閲覧者側で復号化すべきファイルを指定するステップと、

復号化された対称鍵を用いて暗号化したファイルのうち指定された該復号化すべきファイルを復号化するステップとを持つことを特徴とする復号化方法。

【請求項31】 所有者の秘密鍵を用いて前記ファイルの電子署名を生成するステップと、
前記ファイルに該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【請求項32】 所有者の秘密鍵を用いて前記ファイル内容の電子署名を生成するステップと、
前記ファイル内容に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【請求項33】 所有者の秘密鍵を用いて前記ファイルに関する情報の電子署名を生成するステップと、
前記ファイルに関する情報に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【請求項34】 ファイルから電子署名を分離するステップと、

所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【請求項35】 ファイル内容から電子署名を分離するステップと、

所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【請求項36】 ファイルに関する情報から電子署名を分離するステップと、

所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はファイルの送信者が1人又は複数の受信者へ該ファイルを秘密に配布するための暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法に関する。

【0002】

【従来の技術】今日、OA化等により、文書等の電子化が進んでいる。これに伴い重要な電子情報が増えてきており、第三者の不正（盗み見、改ざん、なりすまし）から、守る必要が出てきた。

【0003】上記要望を満たすべく、ファイルに暗号および電子署名処理を施し上記の脅威から守る、ファイル暗号ソフトウェアが現れた。当初、ファイル暗号ソフトウェアは、個人のファイルを守ることをメインに考えら

れていたが、情報化が進み各企業でイントラネット等のネットワーク構築が行われる中、ファイルサーバ上で暗号化されたファイルを共有的に利用するため、ある指定されたグループの人しか見る事ができないというような、グループ暗号の必要性が出てきた。

【0004】グループでのファイル共有を実現するため、現状では以下の方式が用いられている。

(1) 復号時に必要なパスワードをグループで共有するパスワード方式。

【0005】すなわち、送信者はパスワードを用いて暗号ファイルを作成し、当該パスワードをグループの受信者に通知する。グループの受信者は当該パスワードを用いて送信者から送信された暗号ファイルを復号化する。グループ以外の受信者は当該パスワードがないため送信者から送信された暗号ファイルを復号化することができない。

【0006】(2) 復号時に必要なグループ鍵をグループで共有するグループ鍵共有方式。すなわち、送信者はグループ鍵を用いて暗号ファイルを作成し、当該グループ鍵をグループの受信者に通知する。グループの受信者は当該グループ鍵を用いて送信者から送信された暗号ファイルを復号化する。グループ以外の受信者は当該グループ鍵がないため送信者から送信された暗号ファイルを復号化することができない。

【0007】

【発明が解決しようとする課題】パスワード方式では以下のような欠点がある。

(1) グループ全員に暗号ファイルを作成するたびにパスワードを第三者に秘密に配送しなければならない。

【0008】(2) 各暗号ファイル(グループ)ごとにパスワードが増えるので管理が非常に大変である。

(3) どのパスワードがどの暗号ファイルのものか分からなくなる。

【0009】(4) パスワードを忘れてしまう。
また、グループ鍵共有方式では以下のような欠点がある。

(1) 暗号ファイル毎にグループの構成が異なる場合には、グループを構成するたびにグループ鍵を第三者に秘密にグループ全員に配送しなければならない。

【0010】(2) グループを構成するごとにグループ鍵が増えるので管理が非常に大変である。

(3) どのグループ鍵がどのグループのものか分からなくなる。

【0011】(4) グループ鍵を忘れてしまう。
本発明は上記の事情に鑑みてなされたもので、個人が持つ1つの秘密鍵、認証機関(CA)に公開されている1つの公開鍵という形態のまま公開鍵方式のグループ暗号を実現することにより、鍵配送が安全でかつ簡単であり、さらに任意のグループを簡単に作成する事ができる暗号化方法及び装置、復号化方法及び装置、暗号化プロ

グラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法を提供することを目的とする。

【0012】

【課題を解決するための手段】上記目的を達成するために本発明は、ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする。

【0013】また本発明は、ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を記録媒体に記録して受信者へ渡すステップとを少なくとも持つことを特徴とする暗号化方法。

【0014】また本発明は、前記ファイルに関する情報を対称鍵を用いて暗号化するステップを持つことを特徴とする。また本発明は、前記ファイル及びファイルに関する情報に電子署名情報を付与することを特徴とする。

【0015】また本発明は、少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする。また本発明は、暗号化されたファイル又はファイルに関する情報及び対称鍵を復号化する復号化方法であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、該復号化された対称鍵を用いて前記暗号化されたファイル又はファイルに関する情報を復号化するステップとを少なくとも持つことを特徴とする。

【0016】また本発明は、前記復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定するステップを持つことを特徴とする。また本発明は、少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする。

【0017】

【発明の実施の形態】以下図面を参照して本発明の実施の形態例を詳細に説明する。先ず、本発明の実施形態例に表記される記号について説明する。

『公開鍵暗号方式の鍵の表記』

(1) 先頭2文字

PK: 公開鍵

SK: 秘密鍵

(2) 次の1文字

d: 鍵配送に使用する鍵

s : 電子署名に使用する鍵

(3) 4文字目以降

鍵を所持している装置名

(4) 例

PKdA = 装置Aの鍵配送用(d)の公開鍵(PK)

(5) 本発明で使用する鍵

・暗号化装置Aの鍵

PKdA Aの鍵配送用鍵の公開鍵

SKdA Aの鍵配送用鍵の秘密鍵

PKsA Aの電子署名用鍵の公開鍵

SKsA Aの電子署名用鍵の秘密鍵

・復号化装置Bの鍵

PKdB Bの鍵配送用鍵の公開鍵

SKdB Bの鍵配送用鍵の秘密鍵

PKsB Bの電子署名用鍵の公開鍵

SKsB Bの電子署名用鍵の秘密鍵

『関数などの表記』

Cert() : 証明書

(例) Cert(PKdA) = PKdAの証明書

h() : ハッシュ関数

(例) h(M) : 平文Mのハッシュダイジェスト

「電子署名の生成」

(例) SKsA(h(M)) : 平文Mに対するAの電子署名

平文Mのハッシュダイジェストを署名用秘密鍵SKsAで暗号化したもの。

【0018】通常は平文Mに添付し、 $M \parallel SKsA(h(M))$ とする。

「電子署名の検証」

(例) 復号装置が、Aの電子署名付き平文 $M \parallel SKsA(h(M))$ を受け取ったとき、

(1) $M \rightarrow h(M)$: ハッシュ関数を使用

(2) $SKsA(h(M)) \rightarrow h(M)$: 電子署名の復号化

(3) (1)と(2)を比較することが検証に該当し、一致していればOKであり、一致しなければNGである。

【0019】 \parallel : 連結

DEK : セッションキー(Data Encryption Key)であり、平文の暗号化を行う対称鍵方式の対称鍵である。ランダム生成で、通信ごとに使い捨てである。

【0020】Key(M) : 暗号化。「鍵名(暗号化対象)」と書く

[] : 配列

… : 中略

(例) B[i] (i = 1, …, n) : 同様の機能を有するn個の装置

(例) M[j] (j = 1, …, t) : t個の平文M

(例) PKdB[1] (DEK) \parallel … \parallel PKdB

[n] (DEK) : 暗号化して連結したn個のデータ『公開鍵方式について』

「公開鍵には大きく分けて以下の2種類がある。」

(1) RSA等の通常の公開鍵方式

暗号化装置X、復号化装置Yとする。

【0021】暗号化装置Xから復号化装置YへDEKを安全に送信するときの方法は以下になる。暗号化装置Xは、DEKを公開鍵PKdYで暗号化し、PKdY(DEK)となる。一方復号化装置Yは、PKdY(DEK)を秘密鍵SKdYで復号化し、DEKを得る。

【0022】(2) DH・楕円DH等の共有鍵を用いた公開鍵方式

暗号化装置X、復号化装置Yとする。暗号化装置Xから復号化装置YへDEKを安全に送信するときの方法は以下になる。

【0023】暗号化装置Xは、暗号化装置Xの秘密鍵SKdXと復号化装置Yの公開鍵PKdYから共有鍵SXYを生成する。DEKをSXYで暗号化し、SXY(DEK)となる。

【0024】一方、復号化装置Yは、暗号化装置Xの公開鍵PKdXと復号化装置Yの秘密鍵SKdYから共有鍵SYXを生成するが、DH・楕円DH等ではSYX = SXYとなるように秘密鍵と公開鍵が作成されている。

【0025】それゆえ、SYX (= SXY)を生成し、SXY(DEK)を復号化し、DEKを得る。

(3) DHの詳細について

a、pを公開しているとする。aは自然数、pは素数である。

【0026】このとき暗号化装置Xの秘密鍵SKdXと公開鍵PKdXには以下のような関係がある。

$$PKdX = aSKdX \bmod p$$

ここで、modは剰余演算である。

【0027】同様に、復号化装置Yの秘密鍵SKdYと公開鍵PKdYについても、

$$PKdY = aSKdY \bmod p$$

したがって、

$$SXY = PKdY SKdX \bmod p \\ = (aSKdY \bmod p) SKdX \bmod p$$

$$= a(SKdY * SKdX) \bmod p$$

$$SYX = PKdX SKdY \bmod p$$

$$= (aSKdX \bmod p) SKdY \bmod p$$

$$= a(SKdX * SKdY) \bmod p$$

$$= a(SKdY * SKdX) \bmod p = SXY$$

故にSXY = SYXである。

【0028】それゆえ暗号化装置Xと復号化装置Yは同じ共有鍵SXYを公開鍵の交換だけで生成できる。

「公開鍵を用いて暗号化を行うときの表記について」上記のように、公開鍵には

(1) RSA等の通常の公開鍵方式

(2) DH・楕円DH等の共有鍵を用いた公開鍵方式の2種類があり、暗号化の方式が異なる。

【0029】これらの方式の鍵は、方法は異なるが同じ目的(DEKの暗号化・復号化)に用いられる。これらの鍵を同じように扱うため、

DEKの暗号化に用いる鍵を、Enc-X-Y

DEKの復号化に用いる鍵を、Dec-X-Y

と定義する。

・先頭3文字：鍵の種類

Enc：暗号化に使用される鍵

Dec：復号化に使用される鍵

・4文字目は「-」

・5文字目から「-」まで：暗号装置名

・次の「-」から末尾まで：復号装置名

例として、暗号装置Xと復号装置Yの間の鍵について記す。

【0030】(1) では、

EncXY=PKdY

DecXY=SKdY

となり、暗号化装置Xには存在しない鍵となる。

【0031】(2) では、

EncXY=SKdXとPKdYから生成される鍵

DecXY=PKdXとSKdYから生成される鍵

生成元は異なるが、EncXY=DecXYである。

【0032】なお、本発明においては、公開鍵方式として2つの方式を想定しているが、これに限定される必要はなく、他の公開鍵方式でも可能である。また同様に、対称鍵方式についても他の対称鍵方式(共通鍵方式、秘密鍵方式)であってもよい。

【0033】次に、本発明の一実施形態例について説明する。図1は本発明の一実施形態例を示す構成説明図である。図において、101は送信者の暗号化装置Aであり、ファイルを暗号化する。102は受信者の復号化装置B[1]であり、暗号化されたファイルを復号化する。103は受信者の復号化装置B[2]であり、暗号化されたファイルを復号化する。104は受信者の復号化装置B[3]であり、暗号化されたファイルを復号化する。105は認証機関CAであり、暗号化装置A、復号化装置B[1]、復号化装置B[2]、復号化装置B[3]に公開鍵を提供する。

【0034】図2は図1の認証機関CAを介する場合の各装置間の動作フロー図であり、図3は図1の認証機関CAを介さない場合の各装置間の動作フロー図である。すなわち、図2に示すように、ステップ(Step)1において、暗号化装置Aは暗号化装置Aの鍵配送用鍵の公開鍵PKdA、暗号化装置Aの鍵配送用鍵の秘密鍵SKdA、暗号化装置Aの電子署名用鍵の公開鍵PKsA及び暗号化装置Aの電子署名用鍵の秘密鍵SKsAを生成し、このうち公開鍵PKdA及び公開鍵PKsAを認証機関CAに登録する。ステップ2において、認証機関

CAは認証機関CAの証明書を登録する。ステップ3において、復号化装置B[i](i=1, ..., n)は復号化装置B[i]の鍵配送用鍵の公開鍵PKdB[i]及び復号化装置B[i]の電子署名用鍵の公開鍵PKsB[i]を生成し、認証機関CAに登録する。ステップ4において、グループ暗号化を行う前に、暗号化装置Aは認証機関CAに公開鍵PKdB[i]を要求する。ステップ5において、認証機関CAは認証機関CAの証明書を配布する。ステップ6において、認証機関CAは暗号化装置Aに公開鍵PKdB[i]の証明書Cert(PKdB[i])を暗号化装置Aに配布する。ステップ7において、後述する複数人暗号化を行う。ステップ8において、暗号化装置Aは暗号文Cを復号化装置B[i]に配布する。ステップ9において、復号化装置B[i]が暗号文Cを取得・復号化する前に、復号化装置B

[i]は公開鍵PKdA及び公開鍵PKsAを認証機関CAに要求する。ステップ10において、認証機関CAは認証機関CAの証明書を配布する。ステップ11において、認証機関CAは公開鍵PKdAの証明書Cert(PKdA)及び公開鍵PKsAの証明書Cert(PKsA)を復号化装置B[i]に配布する。ステップ12において、後述する複数人復号化を行う。

【0035】また、図3の場合は、ステップ4において、グループ暗号化を行う前に、暗号化装置Aは復号化装置B[i]に必要に応じて公開鍵PKdB[i]を要求する。ステップ6において、暗号化装置Aは復号化装置B[i]から公開鍵PKdB[i]を取得する。ステップ7において、後述する複数人暗号化を行う。ステップ8において、暗号化装置Aは暗号文Cを復号化装置B[i]に配布する。ステップ9において、復号化装置B[i]が暗号文Cを取得・復号化する前に、復号化装置B[i]は必要に応じて公開鍵PKdA及び公開鍵PKsAを暗号化装置Aに要求する。ステップ11において、復号化装置B[i]は公開鍵PKdA及び公開鍵PKsAを暗号化装置Aから取得する。ステップ12において、後述する複数人復号化を行う。

【0036】図4は図2のステップ7に対応した暗号化装置Aの一例を示す構成説明図である。図4の各部を説明する。

(1) ファイル情報分離器601

入力：暗号化するt個のファイルF[j](j=1, ..., t)

出力：ファイル情報M[0]、ファイル内容M[j]

(j=1, ..., t)

ファイルをそれぞれファイル情報(ファイル名、ファイルサイズ、日付、ディレクトリ構造の情報等)とファイル内容(ファイル情報を取り出したファイル中身)に分け、t個のファイル情報をひとつにまとめてM[0]とし、ファイル内容をM[1]、..., M[t](ファイル中身F[1]、..., F[t]に対応)とする。

【0037】(2) グループ情報変換器602、グループ情報DB(データベース)603

入力:暗号化装置利用者名Aまたは復号化装置利用グループ名G(復号装置B[i] (i=1、…、n))

出力:装置名(1以上)A及びB[i] (i=1、…、n)

グループ情報DB603には、利用グループ名(利用者名)と装置名との対応関係が格納されている。このグループ情報DB603の情報を利用して、利用グループ名→利用者名→装置名と変換する。

【0038】(3) 鍵検索器604、鍵DB605

入力:装置名A及びB[i] (i=1、…、n)、要求元(鍵の要求元の情報、複数人暗号器または電子署名生成・連結器の情報)

出力:公開鍵方式の鍵。Aの署名用秘密鍵SKsA、暗号化鍵Enc-A-B[i] (i=1、…、n)

鍵DB605には、装置名とその公開鍵が格納されている。入力を基に、鍵DB605から秘密鍵・公開鍵を取り出して、暗号化鍵を生成し、要求元(複数人暗号器609や電子署名生成・連結器606)へ渡す。本発明ではDHの例を説明する(DHでは暗号化装置の秘密鍵と復号化装置の公開鍵によって暗号化鍵を生成するが、RSA等の公開鍵方式を用いて暗号化鍵を生成する場合は、復号化装置の公開鍵を暗号化鍵として用いる)。

【0039】以降現れる単独のjは、 $0 \leq j \leq t$ のいずれかであり、それぞれの器は、 $t+1$ 回処理を行う。

(4) 乱数発生器607

出力:対称鍵DEK(ランダム生成)

(5) 電子署名生成・連結器606

入力:M[0]又はM[j]、Aの署名用秘密鍵SKsA

出力: $M[j] \parallel SKsA(h(M[j]))$ (j=0、…、t)

ハッシュダイジェスト $h(M[j])$ の生成

電子署名 $SKsA(h(M[j]))$ の生成

$M[j] \parallel SKsA(h(M[j]))$:入力と電子署名の連結

(6) 暗号器608

入力:電子署名付き本文 $M[j] \parallel SKsA(h(M[j]))$ 、対称鍵DEK

出力:暗号化データDEK($M[j] \parallel SKsA(h(M[j]))$) (j=0、…、t)

(7) 複数人暗号器609

入力:対称鍵DEK、複数の暗号化鍵Enc-A-B[i] (i=1、…、n)

出力:暗号化データEnc-A-B[i](DEK) (i=1、…、n)

複数の復号化装置を対象に暗号化する。

【0040】(8) 暗号データ連結器610

入力:全暗号化データDEK($M[j] \parallel SKsA(h$

($M[j])$) (j=0、…、t)及びEnc-A-B[i](DEK) (i=1、…、n)

出力:暗号文C

暗号化データ全てを連結し、一つにまとめる。

【0041】図5は図2のステップ7に対応した暗号化装置Aによるグループ暗号化ファイル作成の一例を示す説明図であり、図6及び図7は図2のステップ7に対応した暗号化装置Aの処理フロー図である。

【0042】すなわち、まず、ファイルの暗号化について説明する。暗号化前にファイルF[j] (j=1、…、t)を選択してファイル情報分離器601に入力する。ファイル情報分離器601は入力されたファイルF[j]をファイル情報M[0]とファイル内容M[j] (j=1、…、t)に分離して電子署名生成・連結器606に出力する。一方、暗号化前に決定済の暗号化装置利用者名Aはグループ情報変換器602に入力され、このグループ情報変換器602はグループ情報DB603を参照して暗号化装置利用者名Aを変換し、暗号化装置名Aを取得して鍵検索器604に出力する。この鍵検索器604は要求元の電子署名生成・連結器606の情報に応じて鍵DB605を参照して暗号化装置名Aの署名用秘密鍵SKsAを検索・取得して電子署名生成・連結器606に出力する。この電子署名生成・連結器606はファイル情報とファイル内容M[j] (j=0、…、t)に電子署名を生成して付加した $M[j] \parallel SKsA(h(M[j]))$ (j=0、…、t)を暗号器608に出力する。この暗号器608には乱数発生器607でランダムに生成された対称鍵DEKが入力され、前記電子署名生成・連結器606から入力された $M[j] \parallel SKsA(h(M[j]))$ (j=0、…、t)を対称鍵DEKで暗号化したファイルの暗号化データDEK($M[j] \parallel SKsA(h(M[j]))$) (j=0、…、t)を暗号データ連結器610に出力する。

【0043】次に、対称鍵の暗号化について説明する。暗号化前に選択済の復号化装置利用グループ名Gはグループ情報変換器602に入力され、このグループ情報変換器602はグループ情報DB603を参照して復号化装置利用グループ名Gを各復号化装置名B[i] (i=1、…、n)へ変換して鍵検索器604に出力する。この鍵検索器604は要求元の複数人暗号器609の情報に応じて鍵DB605を参照して暗号化装置Aと復号化装置B[i] (i=1、…、n)の間の暗号化鍵Enc-A-B[i]を全て検索・取得して複数人暗号器609に出力する。この複数人暗号器609には乱数発生器607でランダムに生成された対称鍵DEKが入力され、この対称鍵DEKを暗号化鍵Enc-A-B[i]で暗号化した対称鍵の暗号化データEnc-A-B[i](DEK)を暗号データ連結器610に出力する。

【0044】前記暗号データ連結器610は暗号器608から入力されたファイルの暗号化データDEK(M

$[j] \parallel SKsA(h(M[j]))$ ($j=0, \dots, t$) 及び複数人暗号器609から入力された対称鍵の暗号化データ $Enc-A-B[i]$ (DEK) 全体を連結し、暗号文Cを生成する。

【0045】図5に示すように、前記ファイル情報M[0]とファイル内容M[j] ($j=1, \dots, t$) は送信者の暗号化装置Aの署名用秘密鍵SKsAで電子署名される。また、電子署名付ファイル情報と電子署名付ファイル内容は対称鍵DEKで暗号化される。さらに、対称鍵DEKは送信者の暗号化装置Aの秘密鍵SKdA及び受信者の復号化装置B[i] ($i=1, \dots, n$) の公開鍵PKdB[i] ($i=1, \dots, n$) を用いて暗号化される。

【0046】尚、暗号化装置Aを復号化対象に含めるか否かは任意である。暗号化装置Aを復号化対象に含めた場合でも、同様に暗号化可能である。B[1]=Aとなる。図8は図2のステップ12に対応した復号化装置B[i] ($i=1, \dots, n$) のファイル情報復号化部分の一例を示す構成説明図である。図8の各部を説明する。

【0047】(1) 暗号データ分離器701

入力：暗号文C

出力：全暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) ($j=0, \dots, t$) 及び $Enc-A-B[i]$ (DEK) ($i=1, \dots, n$)

暗号文Cを(カッコの外の \parallel ごとに)暗号化データに分離する。

【0048】(2) 鍵検索器702、鍵DB703

入力：装置名、要求元(鍵の要求元の情報。複数人復号器704からの暗号化装置名または電子署名分離・検証器706からの要求情報)

出力：公開鍵方式の鍵(複数人復号器704へ復号化鍵 $Dec-A-B[i]$ または電子署名分離・検証器706へ暗号化装置名Aの署名用公開鍵PKsA) 鍵DB703には、装置名とその公開鍵が格納されている。入力を基に、鍵DB703から秘密鍵・公開鍵を取り出して、必要に応じて復号化鍵を生成し、要求元(複数人復号器704や電子署名分離・検証器706)へ渡す。

【0049】(3) 複数人復号器704

入力：暗号化データ $Enc-A-B[i]$ (DEK) ($i=1, \dots, n$) または復号化鍵 $Dec-A-B[i]$

出力：対称鍵DEK

暗号化データ $Enc-A-B[i]$ (DEK) ($i=1, \dots, n$) から、復号化装置B[i] 向けの暗号化データ $Enc-A-B[i]$ (DEK) を選び出し、復号化鍵 $Dec-A-B[i]$ で復号化し、対称鍵DEKを取得する。

【0050】(4) 復号器705

入力：暗号化データDEK ($M[0] \parallel SKsA(h(M[0]))$) および対称鍵DEK

出力：電子署名付き本文 $M[0] \parallel SKsA(h(M$

$[0]))$

(5) 電子署名分離・検証器706

入力：電子署名付き本文 $M[0] \parallel SKsA(h(M[0]))$ 、暗号化装置名Aの署名用公開鍵PKsA

出力：ファイル情報M[0]

$M[0] \parallel SKsA(h(M[0]))$ ：入力と電子署名の分離

ハッシュダイジェスト $h1=h(M[0])$ の生成

$h2=h(M[0])=PKsA(SKsA(h(M[0])))$ ：電子署名 $SKsA(h(M[0]))$ の復号化

署名の検証 ($h1=h2$ かどうか)

$h1=h2 \rightarrow OK$. M[0] を取得

$h1 \neq h2 \rightarrow NG$. 処理を中断

(6) 表示装置708

入力：ファイル情報M[0]

出力：ファイル情報M[0]

復号化するファイル内容M[j]を選択させるため(図9の入力に反映)、ファイル情報M[0]を表示する。

【0051】(7) 一時的記憶装置707

入力：ファイル情報M[0]、対称鍵DEK、暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) ($j=1, \dots, t$)

選択されたファイル内容M[j]を復号化するために必要な、データを格納しておく。

【0052】図9は図2のステップ12に対応した復号化装置B[i] ($i=1, \dots, n$) のファイル内容復号化部分の一例を示す構成説明図である。図9の各部を説明する。

【0053】(1) 入力装置801

入力：インデックス $j[1], \dots, j[u]$ (表示情報から復号化の対象として選択されたファイルの番号)

出力：インデックス $j[1], \dots, j[u]$

表示装置708 (図8参照) の情報を基に、利用者がファイルを選択した結果を得、以降の処理で使用される。

【0054】(2) 一時的記憶装置802 (図8の一時的記憶装置707と同一)

入力：インデックス $j[1], \dots, j[u]$

出力：ファイル情報M[0]、対称鍵DEK、入力装置801で選択されたファイルの番号に対応した暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) ($j=j[1], \dots, j[u]$)

選択されたM[j]を復号化するために必要なデータを他の器へ受け渡す。

【0055】(3) 復号器803

入力：暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) ($j=j[1], \dots, j[u]$) および対称鍵DEK

出力：電子署名付き本文 $M[j] \parallel SKsA(h(M[j]))$ ($j=j[1], \dots, j[u]$)

(4) 鍵検索器805、鍵DB806

入力：装置名（図8で入力済）、要求元（鍵の要求元の情報。電子署名分離・検証器804からの情報）

出力：公開鍵方式の鍵。暗号化装置名Aの署名用公開鍵PKsA

鍵DB806には、装置名とその公開鍵が格納されている。入力を基に、鍵DB806から秘密鍵・公開鍵を取り出して、必要に応じて復号化鍵を生成し、要求元（電子署名分離・検証器804）へ渡す。

【0056】以降現れる単独のjは、j[1]、…、j[u]のいずれか値であり、取り得る値は $1 \leq j \leq t$ である。それぞれの器は、u回処理を行う。

【0057】(5) 電子署名分離・検証器804

入力： $M[j] \parallel SKsA(h(M[j]))$ (j = j[1]、…、j[u])、暗号化装置名Aの署名用公開鍵PKsA

出力：ファイル内容M[j] (j = j[1]、…、j[u])

$M[j]$ 、 $SKsA(h(M[j]))$ ：入力と電子署名の分離

ハッシュダイジェスト $h1 = h(M[j])$ の生成
 $h2 = h(M[j]) = PKsA(SKsA(h(M[j])))$ ：電子署名 $SKsA(h(M[j]))$ の復号化

署名の検証 ($h1 = h2$ か否か)

$h1 = h2 \rightarrow OK$ 、M[j]を取得

$h1 \neq h2 \rightarrow NG$ 、処理を中断もしくはスキップ（次の暗号化データを処理）

(6) ファイル情報連結器807

入力：ファイル情報M[0]およびファイル内容M[j[1]]、…、M[j[u]]

出力：ファイルF[j[1]]、…、F[j[u]]

選択されたファイルのみ、ファイル情報とファイル内容からファイルを再構築する。

【0058】図10は図2のステップ12に対応した復号化装置B[i] (i = 1、…、n) によるグループ暗号化ファイルの復号化の一例を示す説明図であり、図11及び図12は図2のステップ12に対応した復号化装置B[i] (i = 1、…、n) の処理フロー図である。

【0059】すなわち、まず、ファイル情報の復号化について説明する。図8、図10および図11に示すように、暗号データ分離器701は入力された暗号文Cを暗号化部分ごとに分離し、全暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) (j = 0、…、t) 及びEnc-A-B[i] (DEK) (i = 1、…、n) を取得し、暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) (j = 1、…、t) は一時的記憶装置707に格納し、暗号化データEnc-A-B[i] (DEK) (i = 1、…、n) は複数人復号器704に出力し、暗号化データDEK ($M[0] \parallel SKs$

$A(h(M[0]))$) は復号器705に出力する。複数人復号器704は鍵検索器702、鍵DB703に要求して暗号化装置Aと復号化装置B[i] の間の復号化鍵Dec-A-B[i] を検索、取得し、暗号化データEnc-A-B[i] (DEK) を復号化鍵Dec-A-B[i] で復号化し、対称鍵DEKを取得し、この対称鍵DEKを一時的記憶装置707に格納すると共に復号器705に出力する。この復号器705は暗号化データDEK ($M[0] \parallel SKsA(h(M[0]))$) を対称鍵DEKで復号化し、 $M[0] \parallel SKsA(h(M[0]))$ ($M[0]$ とAの電子署名) を取得し、電子署名分離・検証器706に出力する。電子署名分離・検証器706は鍵検索器702、鍵DB703に要求して暗号化装置Aの署名用公開鍵PKsAを検索、取得する。電子署名分離・検証器706は $SKsA(h(M[0]))$ (Aの電子署名) を検証し、電子署名が間違っていれば(NG)、エラー処理し、処理を中断する。一方、電子署名が正しければ(OK)、ファイル情報M[0]を取得し、このファイル情報M[0]を一時的記憶装置707に格納すると共に表示装置708に出力する。表示装置708はファイル情報M[0]を表示して出力する。

【0060】次に、ファイル内容の復号化について説明する。図9、図10および図12に示すように、入力装置801には表示装置708（図8参照）に表示されているファイル情報M[0]を基にしてファイルの番号であるインデックスj[1]、…、j[u]が選択されて入力され、このインデックスj[1]、…、j[u]は一時的記憶装置802に出力される。この一時的記憶装置802には一時的記憶装置707（図8参照）と同様にファイル情報M[0]、暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) (j = 1、…、t)、及び対称鍵DEKが格納されており、前記ファイル情報M[0]は読み出されてファイル情報連結器807に出力され、前記暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) (j = 1、…、t)、及び対称鍵DEKは読み出されて復号器803に出力される。この復号器803は暗号化データDEK ($M[j] \parallel SKsA(h(M[j]))$) (j = 1、…、t) を対称鍵DEKで復号化し、 $M[j] \parallel SKsA(h(M[j]))$ ($M[j]$ とAの電子署名) を取得して電子署名分離・検証器804に出力する。電子署名分離・検証器804は鍵検索器805、鍵DB806に要求して暗号化装置Aの署名用公開鍵PKsAを検索、取得する。前記電子署名分離・検証器804は $SKsA(h(M[j]))$ (Aの電子署名) を検証し、電子署名が間違っていれば(NG)、エラー処理し、処理を中断もしくはスキップして次のM[j]に対する処理を行う。一方、電子署名が正しければ(OK)、ファイル内容M[j] (j = j[1]、…、j[u]) を取得してファ

イル情報連結器807に出力する。このファイル情報連結器807はファイル情報M[0]及びファイル内容M[j] (j=j[1], ..., j[u]) からファイルF[j] (j=j[1], ..., j[u]) を生成して出力する。

【0061】図10に示すように、暗号化された対称鍵DEKは送信者の暗号化装置Aの公開鍵(楕円DH)PKdA及び受信者の復号化装置B[i] (i=1, ..., n)の秘密鍵SKdB[i] (i=1, ..., n)を用いて復号化される。また、暗号化された電子署名付ファイル情報とファイル内容は対称鍵DEKで復号化される。さらに、電子署名付ファイル情報と電子署名付ファイル内容は送信者の暗号化装置Aの署名用公開鍵PKsAで電子署名が分離・検証される。

【0062】尚、送信者が暗号化したファイルと暗号化した対称鍵を記録媒体に記録して受信者に渡すようにしてもよい。又、少なくとも公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するようにしてもよい。

【0063】本発明の実施形態には次の発明が含まれる。

(1) ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする暗号化方法。

【0064】(2) ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を記録媒体に記録して受信者へ渡すステップとを少なくとも持つことを特徴とする暗号化方法。

【0065】(3) 前記ファイルに関する情報を対称鍵を用いて暗号化するステップを持つことを特徴とする上記(1)又は(2)記載の暗号化方法。

(4) 前記ファイル内容及びファイルに関する情報に電子署名情報を付与することを特徴とする上記(3)記載の暗号化方法。

【0066】(5) 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする上記(1)、(2)、(3)又は(4)記載の暗号化方法。

【0067】(6) 暗号化されたファイル及び対称鍵を復号化する復号化方法であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、該

復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。

【0068】(7) 暗号化されたファイル及び対称鍵を復号化する復号化方法であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、該復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップと、復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定するステップを持つことを特徴とする復号化方法。

【0069】(8) 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする上記(6)又は(7)記載の復号化方法。

【0070】(9) 対称鍵を発生する対称鍵発生手段と、この対称鍵発生手段で発生した対称鍵でファイルを暗号化するファイル暗号化手段と、前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルを連結する連結手段とを具備することを特徴とする暗号化装置。

【0071】(10) 対称鍵を発生する対称鍵発生手段と、この対称鍵発生手段で発生した対称鍵でファイルを暗号化するファイル暗号化手段と、前記対称鍵発生手段で発生した対称鍵でファイルに関する情報を暗号化するファイル情報暗号化手段と、前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルと前記ファイル情報暗号化手段で暗号化したファイルに関する情報を連結する連結手段とを具備することを特徴とする暗号化装置。

【0072】(11) ファイル内容及びファイルに関する情報に送信者の署名用秘密鍵で電子署名情報を付与する電子署名手段を具備することを特徴とする上記(9)又は(10)記載の暗号化装置。

【0073】(12) 暗号データから暗号化された対称鍵と暗号化されたファイルを分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。

【0074】(13) 暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用



いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、このファイル復号化手段で復号化された電子署名付ファイルを送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。

【0075】(14) 暗号データから暗号化された対称鍵と暗号化されたファイルに関する情報と暗号化されたファイル内容を分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイル情報を復号化するファイル情報復号化手段と、前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。

【0076】(15) 暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルに関する情報と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイル情報を復号化するファイルに関する情報復号化手段と、前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、このファイル復号化手段で復号化された電子署名付ファイルと前記ファイル情報復号化手段で復号化された電子署名付ファイル情報を送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。

【0077】(16) 復号化されたファイル情報に基づいて所定のファイルを選択して復号化するファイル選択手段を具備することを特徴とする上記(14)又は(15)記載の復号化装置。

【0078】(17) ファイルの送信者が1人又は複数の受信者へ該ファイルを配布するための暗号化プログラムを記録した記録媒体であって、対称鍵を用いて該ファイルを暗号化する手順、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化する手順、前記暗号化したファイルと前記暗号化した対称鍵を送信する手順を実行させるための暗号化プログラムを記録した記録媒体。

【0079】(18) 前記ファイルに関する情報を対称鍵を用いて暗号化する手順を実行させるためのプログラムを記録したことを特徴とする上記(17)記載の暗

号化プログラムを記録した記録媒体。

【0080】(19) 前記ファイル及びファイルに関する情報に電子署名情報を付与するためのプログラムを記録したことを特徴とする上記(18)記載の暗号化プログラムを記録した記録媒体。

【0081】(20) 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする上記(17)、(18)、又は(19)記載の暗号化プログラムを記録した記録媒体。

【0082】(21) 暗号化されたファイル内容又はファイルに関する情報及び対称鍵を復号化するためのプログラムを記録した記録媒体であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化する手順、該復号化された対称鍵を用いて前記暗号化されたファイル内容又はファイルに関する情報を復号化する手順を実行させるための復号化プログラムを記録した記録媒体。

【0083】(22) 前記復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定する手順を実行させるためのプログラムを記録したことを特徴とする上記(21)記載の復号化プログラムを記録した記録媒体。

【0084】(23) 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする上記(21)又は(22)記載の復号化プログラムを記録した記録媒体。

【0085】(24) ファイルの所有者が複数の閲覧者(所有者を含む)へ該ファイルを暗号化する方法であって、対称鍵を用いて前記ファイルを暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【0086】(25) ファイルの所有者が複数の閲覧者(所有者を含む)へファイルの内容と該ファイルに関する情報を暗号化する方法であって、該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【0087】(26) ファイルの所有者が複数の閲覧者(所有者を含む)へ該ファイルを暗号化する方法であって、前記所有者が前記閲覧者の情報を任意のグループ

に分けて管理するステップと、該グループから、前記グループに属する閲覧者の情報を抽出するステップと、前記閲覧者の情報から前記閲覧者の公開鍵を抽出するステップと、対称鍵を用いて前記ファイルを暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【0088】(27) ファイルの所有者が複数の閲覧者(所有者を含む)へファイル内容と該ファイルに関する情報を暗号化する方法であって、前記所有者が前記閲覧者の情報を任意のグループに分けて管理するステップと、該グループから、前記グループに属する閲覧者の情報を抽出するステップと、前記閲覧者の情報から前記閲覧者の公開鍵を抽出するステップと、該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【0089】(28) 暗号化したファイルと暗号化済対称鍵全てを結合したものを復号化する方法であって、前記暗号化したファイルと暗号化済対称鍵全てを結合したものから、前記暗号化したファイルと暗号化済対称鍵全てを分離するステップと、所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、該復号化された対称鍵を用いて該暗号化したファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。

【0090】(29) 暗号化したファイル内容と暗号化したファイルに関する情報と暗号化済対称鍵全てを結合したものを復号化する方法であって、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と暗号化済対称鍵全てを分離するステップと、所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、該復号化された対称鍵を用いて該暗号化したファイル内容と該暗号化したファイルに関する情報を復号化するステップと、該復号化されたファイル内容と該復号化されたファイルに関する情報を結合し前記ファイルを再構成するステップとを少なくとも持つことを特徴とする復号化方法。

【0091】(30) 復号化されたファイルに関する情報に基き、閲覧者側で復号化すべきファイルを指定す

るステップと、復号化された対称鍵を用いて暗号化したファイルのうち指定された該復号化すべきファイルを復号化するステップとを持つことを特徴とする復号化方法。

【0092】(31) 所有者の秘密鍵を用いて前記ファイルの電子署名を生成するステップと、前記ファイルに該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【0093】(32) 所有者の秘密鍵を用いて前記ファイル内容の電子署名を生成するステップと、前記ファイル内容に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【0094】(33) 所有者の秘密鍵を用いて前記ファイルに関する情報の電子署名を生成するステップと、前記ファイルに関する情報に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【0095】(34) ファイルから電子署名を分離するステップと、所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【0096】(35) ファイル内容から電子署名を分離するステップと、所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【0097】(36) ファイルに関する情報から電子署名を分離するステップと、所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【0098】

【発明の効果】以上述べたように本発明によれば、個人が持つ1つの秘密鍵、認証機関(CA)に公開されている1つの公開鍵という形態のままで公開鍵方式のグループ暗号を実現することにより、鍵配送が安全でかつ簡単であり、さらに任意のグループを簡単に作成する事ができる暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法を提供することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態例を示す概略構成説明図である。

【図2】本発明の一実施形態例に係る認証機関を介する場合の各装置間のフロー図である。

【図3】本発明の一実施形態例に係る認証機関を介さない場合の各装置間のフロー図である。

【図4】本発明の一実施形態例に係る暗号化装置を示す構成説明図である。

【図5】本発明の一実施形態例に係る暗号化装置のグループ暗号化ファイル作成を示す説明図である。

【図6】本発明の一実施形態例に係る暗号化装置の暗号

化ファイル作成を示すフロー図である。

【図7】本発明の一実施形態例に係る暗号化装置の暗号化対称鍵作成を示すフロー図である。

【図8】本発明の一実施形態例に係る復号化装置のファイル情報復号化部分を示す構成説明図である。

【図9】本発明の一実施形態例に係る復号化装置のファイル内容復号化部分を示す構成説明図である。

【図10】本発明の一実施形態例に係る復号化装置のグループ復号化ファイル作成を示す説明図である。

【図11】本発明の一実施形態例に係る復号化装置のファイル情報復号化部分を示すフロー図である。

【図12】本発明の一実施形態例に係る復号化装置のファイル内容復号化部分を示すフロー図である。

【符号の説明】

101 送信者の暗号化装置A

102 受信者の復号化装置B〔1〕

103 受信者の復号化装置B〔2〕

104 受信者の復号化装置B〔3〕

105 認証機関CA

601 ファイル情報分離器

602 グループ情報変換器

603 グループ情報DB

604 鍵検索器

605 鍵DB

606 電子署名生成・連結器

607 乱数発生器

608 暗号器

609 複数人暗号器

610 暗号データ連結器

701 暗号データ分離器

702 鍵検索器

703 鍵DB

704 複数人復号器

705 復号器

706 電子署名分離・検証器

707 一時的記憶装置

708 表示装置

801 入力装置

802 一時的記憶装置

803 復号器

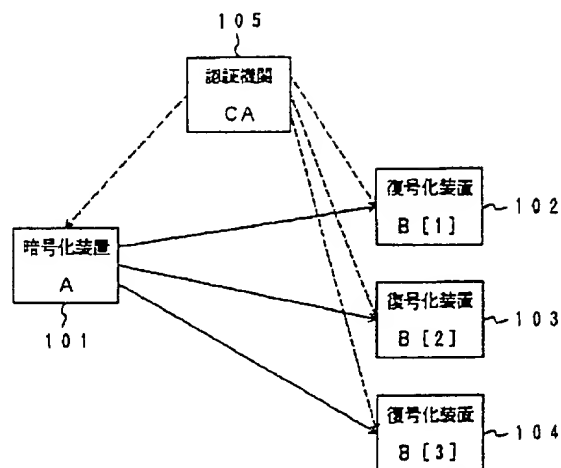
804 電子署名分離・検証器

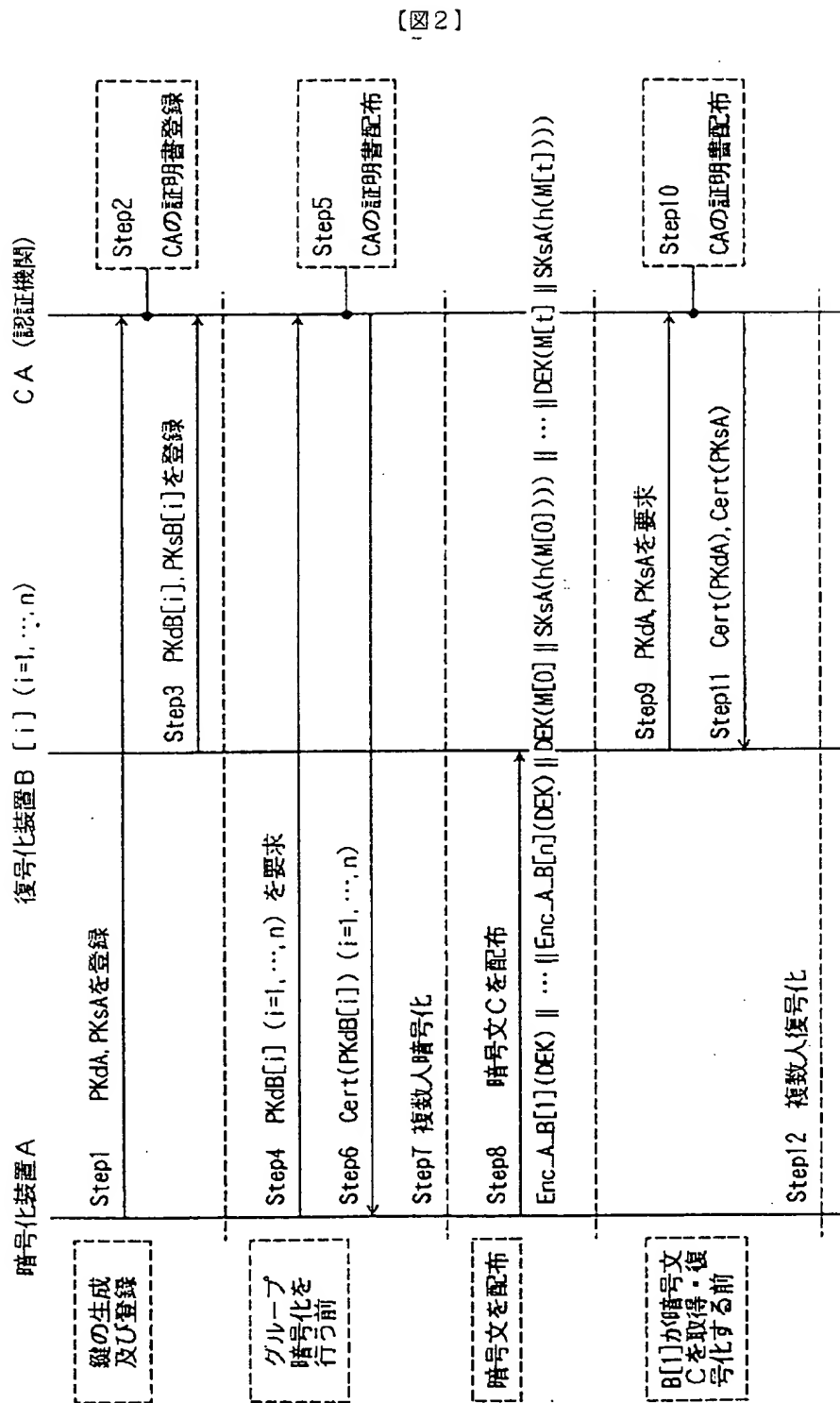
805 鍵検索器

806 鍵DB

807 ファイル情報連結器

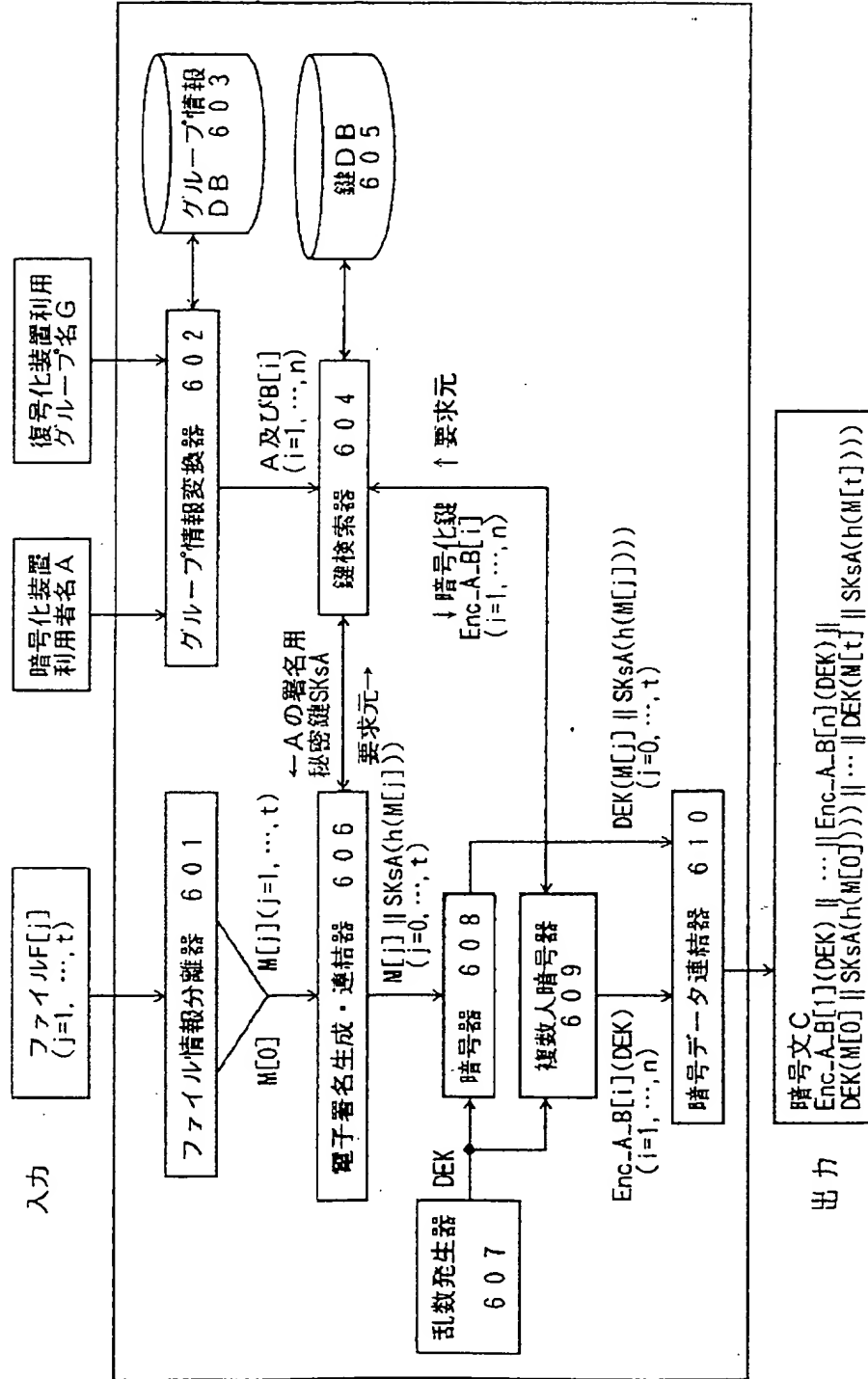
【図1】



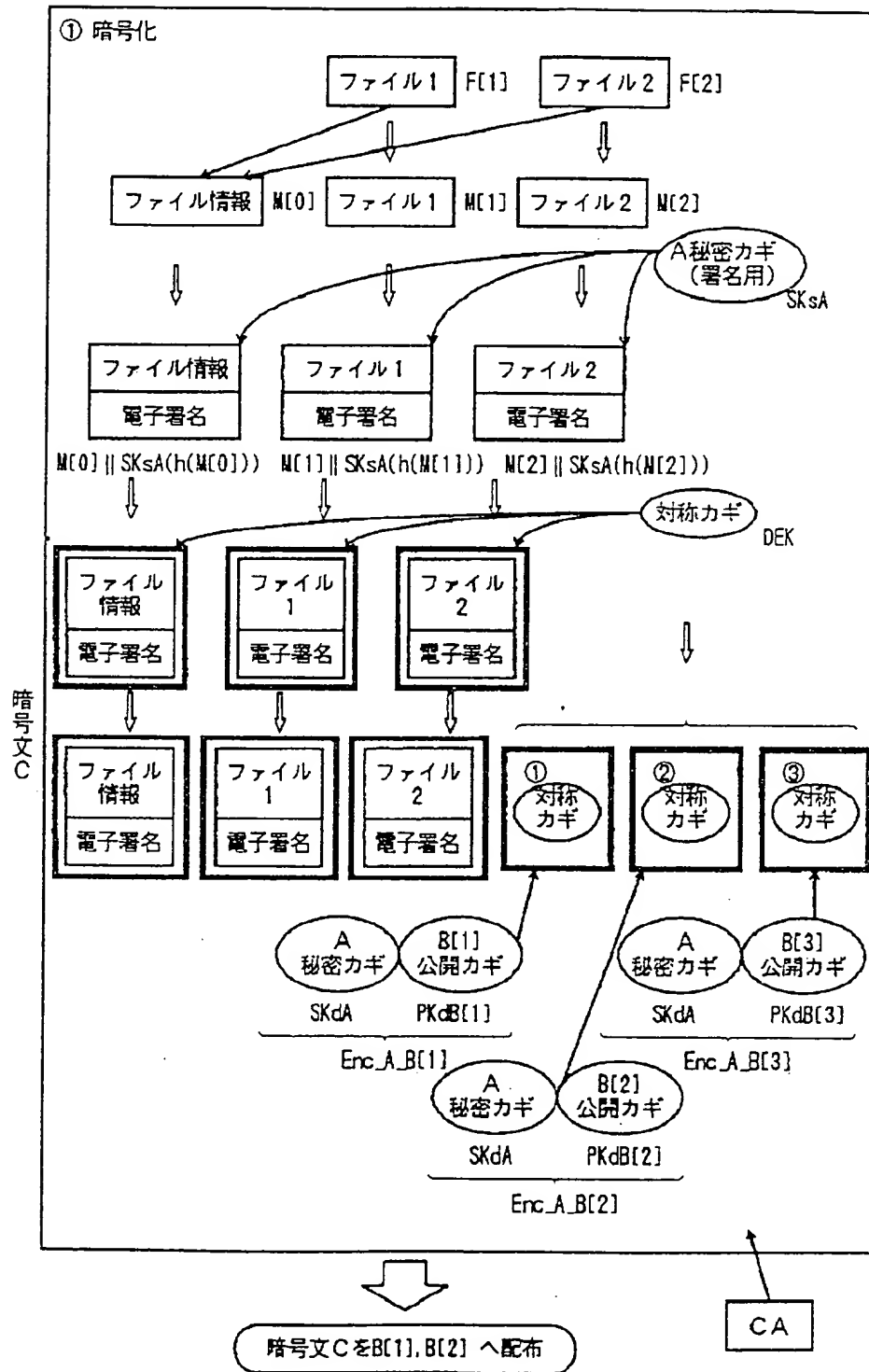


【図2】

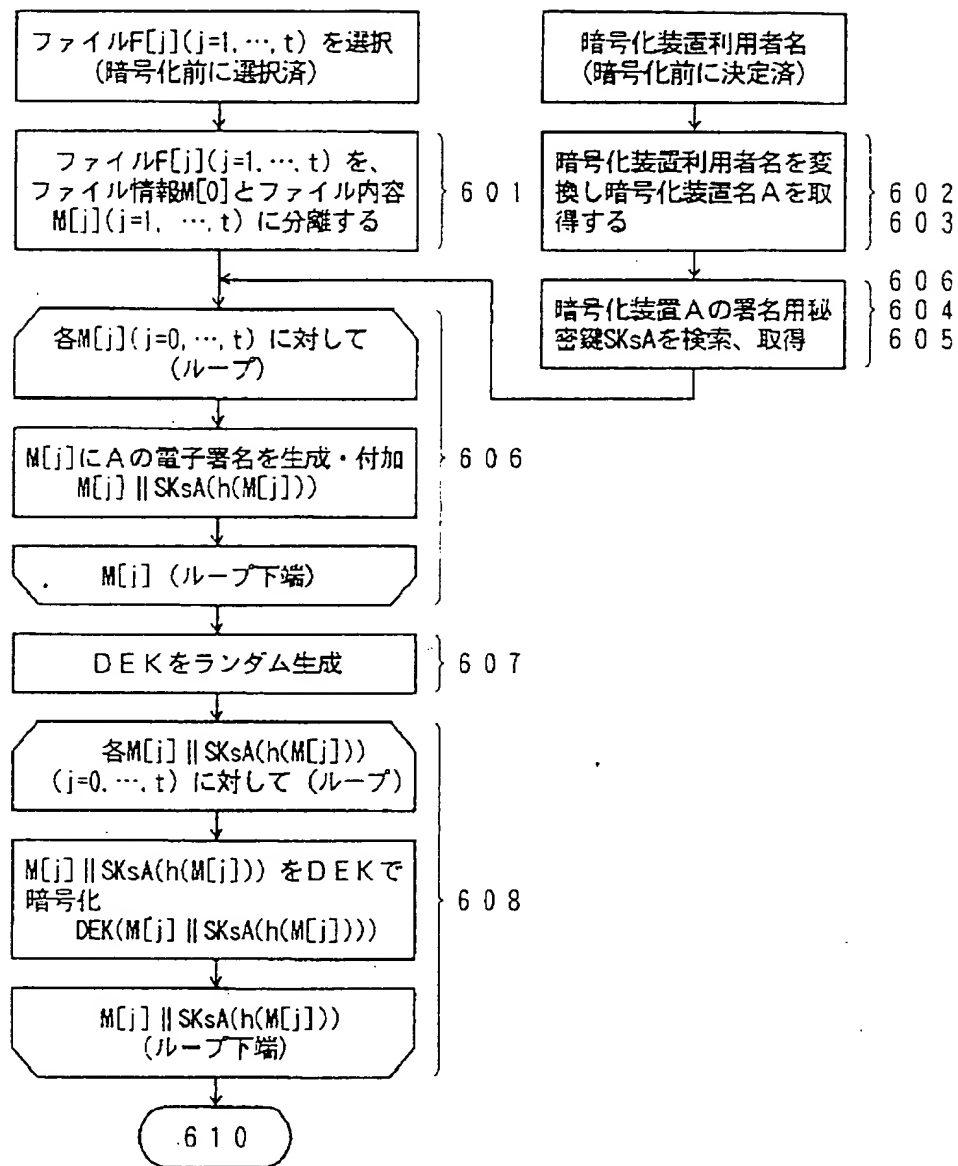
【図4】



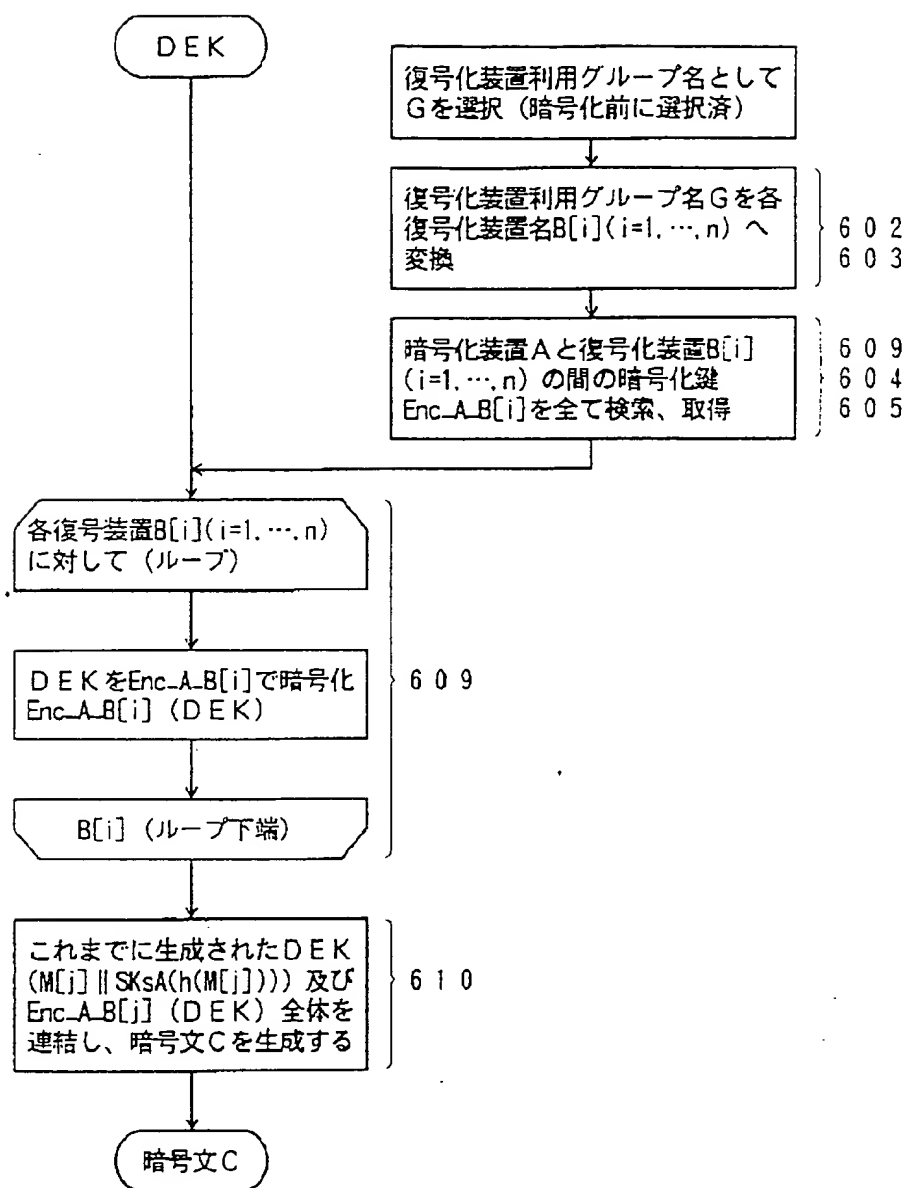
【図5】



【図6】

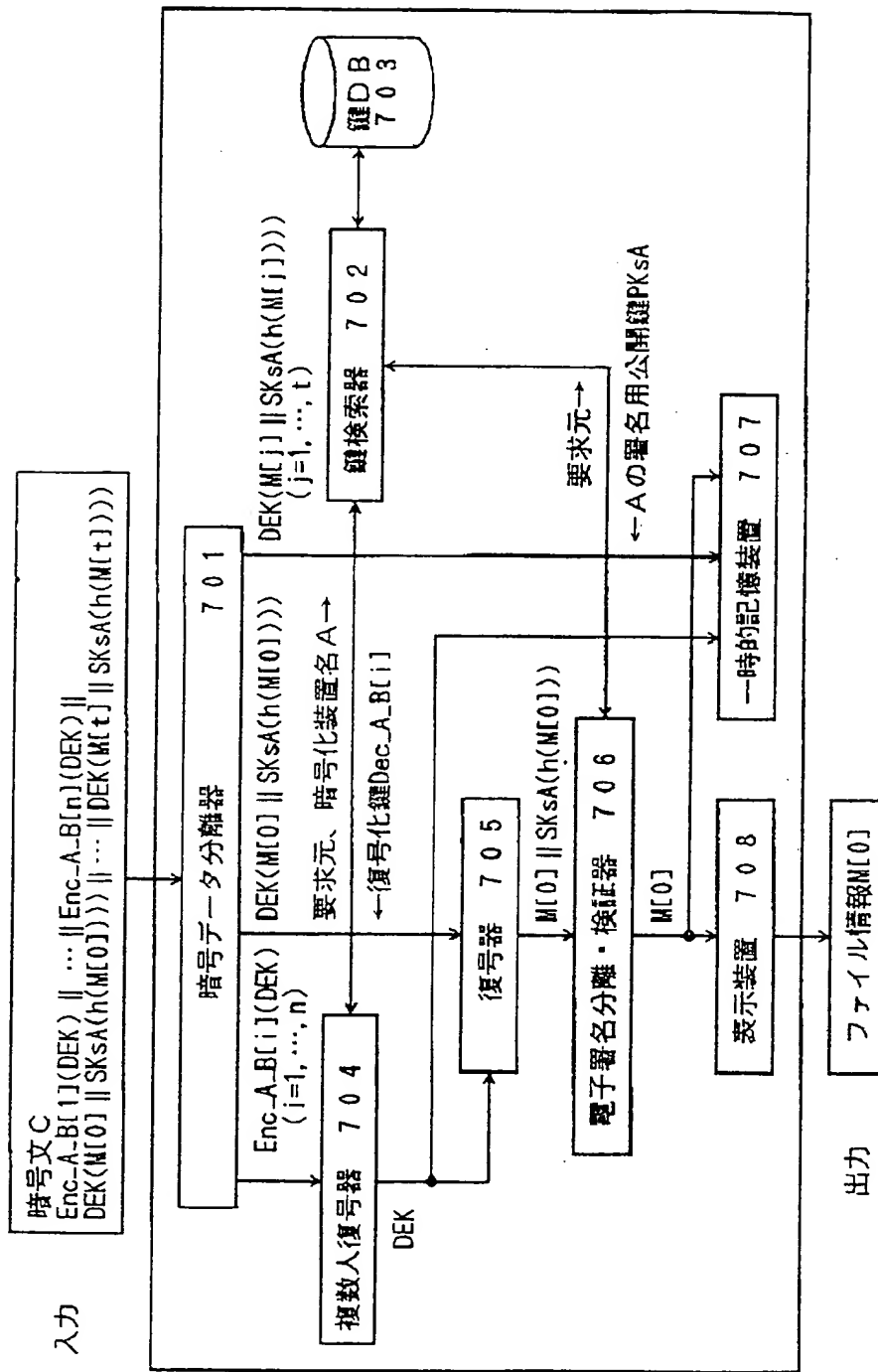


【図7】

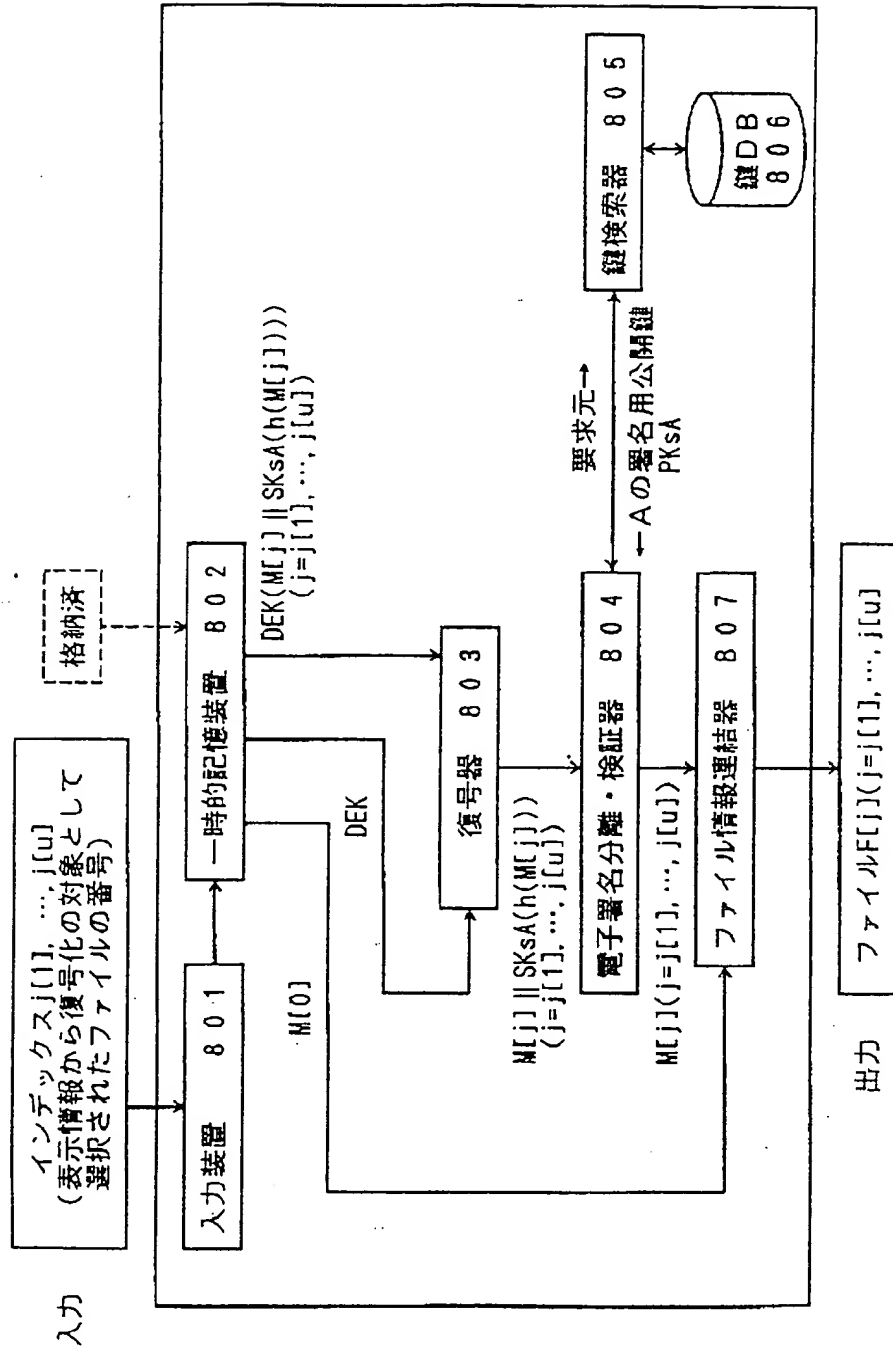


暗号文Cの内容

$Enc_A_B[1](DEK) || \dots || Enc_A_B[n](DEK) ||$
 $DEK(M[0] || SKsA(h(M[0]))) || \dots || DEK(M[t] || SKsA(h(M[t])))$

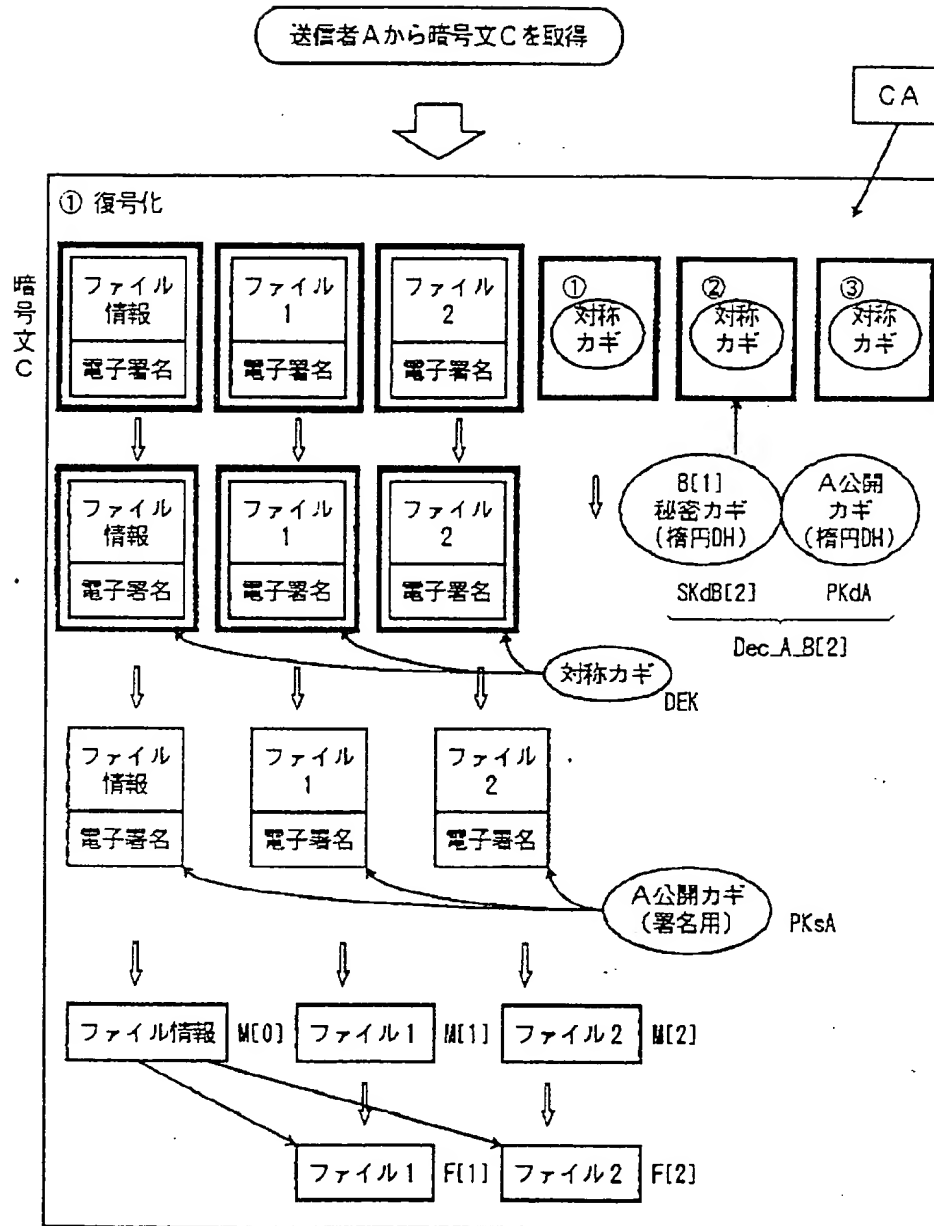


【図 8】

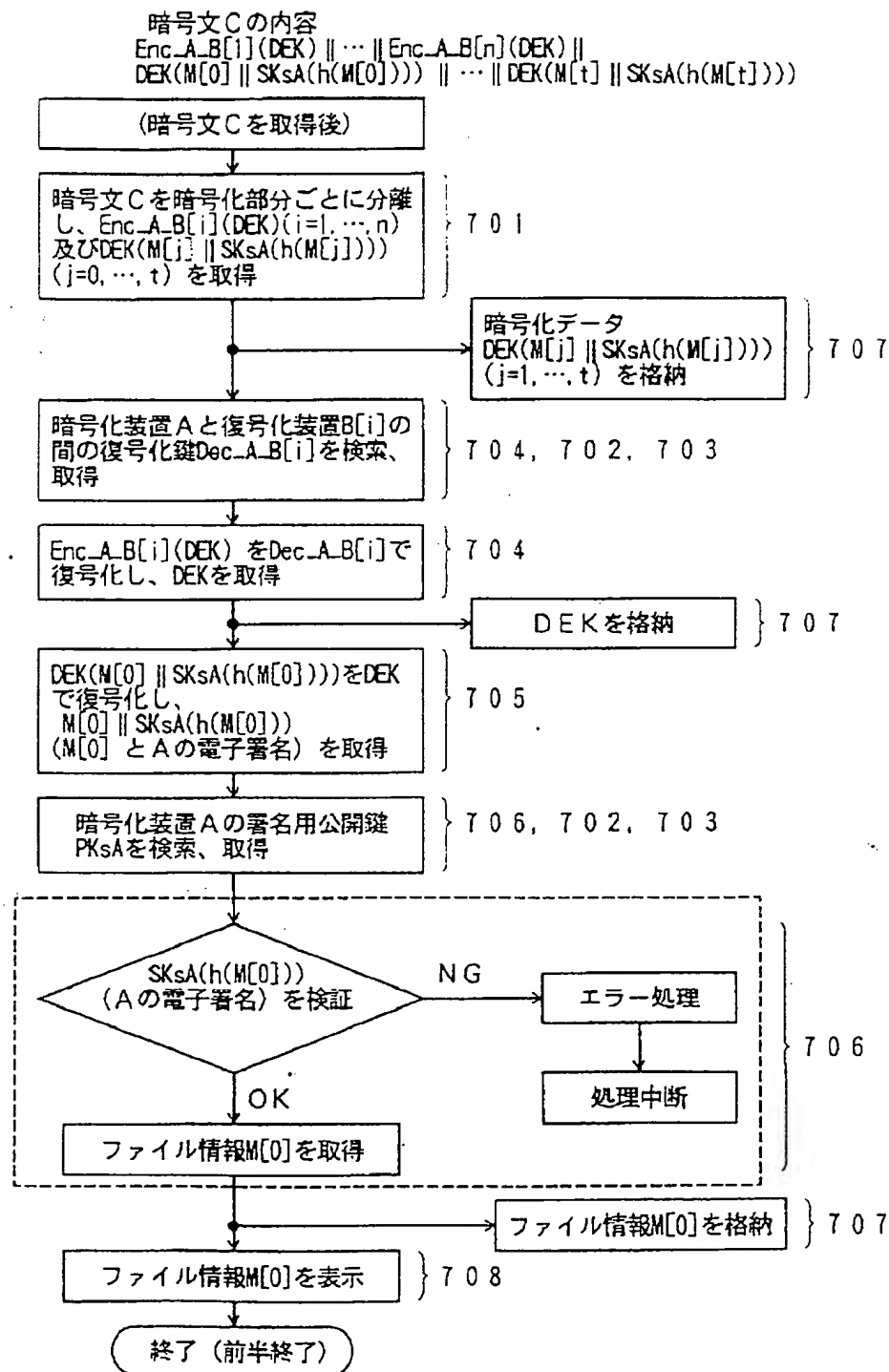


【図9】

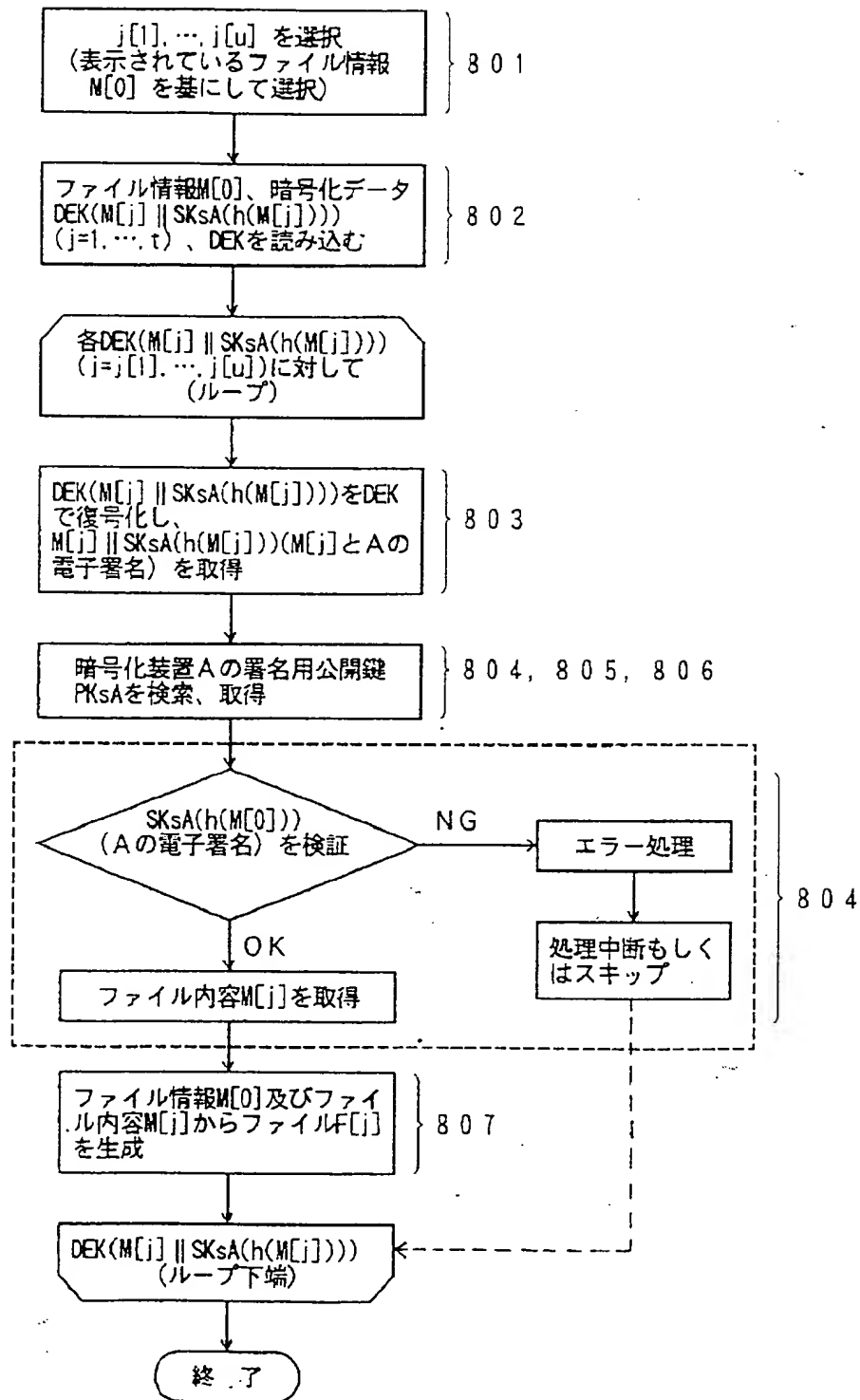
【図10】



【図11】



【図12】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.